06-05-00

A

Please type a plus sign (+) inside this box [+]

PTO/SB/05 (12/97)
Approved for use through 09/30/00. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. 042390.P8731 Total Pages 2

First Named Inventor or Application Identifier Donald D. Baumann

Express Mail Label No. EL143571250US

ADDRESS TO:	**Assistant Commissioner for Patents** **Box Patent Application** **Washington, D. C. 20231**

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. [X] Fee Transmittal Form
   (Submit an original, and a duplicate for fee processing)

2. [X] Specification (Total Pages 23)
   (preferred arrangement set forth below)
   - Descriptive Title of the Invention
   - Cross References to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to Microfiche Appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings (if filed)
   - Detailed Description
   - Claims
   - Abstract of the Disclosure

3. [X] Drawings(s) (35 USC 113) (Total Sheets 6)

4. [X] Oath or Declaration (Total Pages 5) **unsigned**
   a. [ ] Newly Executed (Original)
   b. [ ] Copy from a Prior Application (37 CFR 1.63(d))
   (for Continuation/Divisional with Box 17 completed) **(Note Box 5 below)**
   i. [ ] DELETIONS OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).

5. [ ] Incorporation By Reference (useable if Box 4b is checked)
   The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. ____ Microfiche Computer Program (Appendix)

7. ____ Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. ____ Computer Readable Copy
b. ____ Paper Copy (identical to computer copy)
c. ____ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. ____ Assignment Papers (cover sheet & documents(s))

9. ____ a. 37 CFR 3.73(b) Statement (where there is an assignee)

____ b. Power of Attorney

10. ____ English Translation Document (if applicable)

11. ____ a. Information Disclosure Statement (IDS)/PTO-1449

____ b. Copies of IDS Citations

12. ____ Preliminary Amendment

13. X Return Receipt Postcard (MPEP 503) (Should be specifically itemized)

14. ____ a. Small Entity Statement(s)

____ b. Statement filed in prior application, Status still proper and desired

15. ____ Certified Copy of Priority Document(s) (if foreign priority is claimed)

16. ____ Other: _____

_____

_____

_____

17. **If a CONTINUING APPLICATION,** check appropriate box and supply the requisite information:

____ Continuation ____ Divisional ____ Continuation-in-part (CIP)

of prior application No: _____

18. **Correspondence Address**

____ Customer Number or Bar Code Label _____
(Insert Customer No. or Attach Bar Code Label here)

or

X Correspondence Address Below

NAME Edwin H. Taylor, Reg. No. 25,129

ADDRESS BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

12400 Wilshire Boulevard, Seventh Floor

CITY Los Angeles STATE California ZIP CODE 90025-1026

Country U.S.A. TELEPHONE (408) 720-8598 FAX (408) 720-9397

UNITED STATES PATENT APPLICATION

for

METHOD FOR THEFT DETECTION AND NOTIFICATION VIA A NETWORK

Inventors:

Thomas L. Stachura
Anil Vasudevan

PREPARED BY:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026
(408) 720-8598

File No: 42390.P8731

METHOD FOR THEFT DETECTION AND NOTIFICATION VIA A NETWORK

FIELD OF THE INVENTION

This invention relates to technologies in theft detection and notification generally and particularly to technologies in preventing theft of and tracking properties of an organization.

BACKGROUND OF THE INVENTION

Theft of information processing apparatus, such as a computer system, and its components, such as its processors, add-on cards, etc., continue to plague businesses today. Although many theft preventive measures exist today, none provides a cost-effective mechanism for an organization to both deter the theft of its properties and to track their whereabouts when stolen.

For example, one conventional mechanism involves physically chaining an information processing apparatus, such as a notebook computer, to fixtures of an organization. Specifically, each notebook computer has an associated docking station. Each docking station has a locking mechanism to secure the notebook computer to the station. Then a wire lock fastens the station to a company fixture, such as a desk. One shortcoming of this method is its inability to relocate the notebook computer once it leaves the physical premises of the organization. Also, the method is likely to be an expensive proposition for an organization with a large number of notebook computers. First, the organization needs to purchase a docking station and an appropriate wire lock for each notebook computer that it owns. Second, the organization may also need to hire additional resources to properly deploy such a theft preventive mechanism throughout the organization.

Another common theft preventive mechanism involves attaching theft detection tags to the properties of an organization. Usually, only authorized personnel of the organization has access to special tools that can easily remove or desensitize these tags. In addition, the organization strategically places sensing devices near the exits of its physical premises. Thus, if a property of the organization, having an attached and still sensitized tag, is brought near or past the sensing device, the sensing device alerts the security personnel of the organization. However, this method is susceptible to individuals removing or desensitizing the theft detection tags, and lacks any recovery mechanism after the property leaves the organization's physical premises.

Therefore, an improved method and apparatus is needed to address the discussed issues and still provide a cost-effective theft detection and notification solution.

SUMMARY OF THE INVENTION

A method and apparatus for preventing theft of an organization property is disclosed.

In one embodiment, the method and apparatus authenticates the ownership of an organization property by comparing stored identification information with collected identification information of the organization property. Then the method and apparatus transmits multiple types of network packets containing such authentication result to organization servers via a network.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and is not limited by the figures of the accompanying drawings, in which like references indicate similar elements, and in which:

Figure 1(a) illustrates a general block diagram of one embodiment of a theft prevention system in one network configuration.

Figure 1(b) illustrates a general block diagram of another embodiment of a theft prevention system in one network configuration.

Figure 2 demonstrates a general block diagram of an intranet server.

Figure 3 illustrates a general purpose computer system.

Figure 4 illustrates a flow chart of one process that one embodiment of a theft prevention system follows.

Figure 5 illustrates a flow chart of one process that one embodiment of a theft monitor follows.

DETAILED DESCRIPTION

A method and an apparatus for preventing theft of an organization property is disclosed. In the following description, numerous specific details such as theft scenario 1 and 2, processor P, validation system V and notebook computer N are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one of ordinary skill in the art that the invention may be practiced without these particular details. In other instances, well-known elements and theories, such as the Internet, intranet, client-server architecture, Transmission Control Protocol/Internet Protocol (hereinafter TCP/IP), database technology, network packets, etc. have not been discussed in special details in order to avoid obscuring the present invention.

Moreover, the term "organization" broadly refers to a number of persons or groups united for a particular purpose. Some examples of an organization are, but not limited to, a family, a group, a department, a division or a company. Any property owned by an organization is referred as an "organization property". Also throughout the following discussions, the terms, "packet" and "network packet", are used interchangeably. Additionally, the illustrative examples of the present invention refer to some other noteworthy terms. One such term is an Internet Protocol address (hereinafter IP address), which refers to an identifier for a computer or device on a TCP/IP network. Another term "subnet" refers to a portion of a

network that shares a common address component. In TCP/IP context, two devices are considered to be on the same subnet when their IP addresses have the same prefixes. Yet another term "firewall systems" refers systems designed to prevent unauthorized users from accessing private networks. Finally, a machine readable medium refers to, but not limited to, a storage device, a memory device, a carrier wave, etc.

Figure 1(a) illustrates a general block diagram of one embodiment of a theft prevention system that monitors organization property 102. Organization property 102 can be, but not limited to, a desktop computer system, a notebook computer system or any electronic system owned by organization 100. The system utilizes one network configuration, which includes private network 114, firewall system 116 and outside network 118. Private network 114, as an internal network of organization 100, may operate any number of well-known or proprietary network protocols. Together with firewall system 116, private network 114 is most likely accessible only to authorized personnel of organization 100. On the other hand, outside network 118 connects organization 100 to other organizations such as third party organization 120. One example of outside network 118 is the Internet.

Moreover, this embodiment of the theft prevention system includes, but not limited to, tamper-resistant storage 104, theft monitor 106, intranet server 110 and internet server 112. Tamper-resistant storage 104 refers to a storage medium that is

difficult for unauthorized individuals to make modifications to. For instance, organization 100 may program certain information in storage devices such as a flash memory or a one-time programmable memory so that the stored information is difficult to tamper with. Alternatively, tamper-resistant storage 104 may also refer to an ordinary storage device, such as a disk driver, where one ordinarily skilled in the art opts to encrypt and store sensitive information in obscure locations of the device.

Tamper-resistant storage 104 typically stores identification information that pertains to organization 100's ownership of organization property 102. Subsequent discussions refer to this identification information as "stored identification information". Some examples of the stored identification information are, but not limited to, an IP address, subnet information, serial numbers, device identification numbers, network addresses of intranet server 110 and internet server 112, etc.

One embodiment of theft monitor 106 accesses tamper-resistant storage 104 and applies the stored identification information to authenticate the ownership of organization property 102. Specifically, theft monitor 106 first collects identification information from organization property 102. Subsequent discussions refer to this information as "collected identification information". The collected identification information not only includes the same type of information as the stored identification information, but may also comprise further information

reflective of the identity of organization property 102's user or the location of organization property 102. Then theft monitor 106 compares the two types of identification information and transmits the comparison result and any other relevant identification information to intranet server 110 or internet server 112. It is important to note that one ordinarily skilled in the art may implement the described functionality of theft monitor 106 either in hardware or in software without exceeding the scope of the present invention.

Aside from this described system-level monitoring, another embodiment of a theft prevention system is capable of conducting component-level monitoring as shown in Figure 1(b). In particular, still utilizing tamper-resistant storage 104, theft monitor 106, intranet server 110 and internet server 112, this system mainly monitors organization property 102", which represents components of a system. For instance, organization property 102" can be, but not limited to, a processor, an add-in card, etc. of electronic system 124. Also, theft monitor 106 in Figure 1(b) mainly derives the collected identification information from electronic system 124.

As shown in both Figure 1(a) and Figure 1(b), theft monitor 106 communicates with intranet server 110 and internet server 112 through network access controller 108 and 108", respectively. One ordinarily skilled in the art should note that these network access controllers provide connectivity services for various

types of communication mediums, such as copper wire, lasers, microwaves, communication satellites, etc.

Furthermore, intranet server 110 refers to a server system that provides services to client systems, such as organization property 102 and electronic system 124, that are connected to private network 114. Figure 2 illustrates a general block diagram of one intranet server 110. Particularly, intranet server 110 receives and transmits information from and to private network 114 through network interface 204. Server core 200 fields requests from client systems connected to private network 114 and invokes appropriate programs residing on the server system to respond to such requests. Policy engine 202, which can be a part of or an extension of server core 200, analyzes information from theft monitor 106, attempts to establish whether theft has occurred and provides recovery guidelines for organization 100 to follow. Policy engine 202 also accesses inventory information, scheduling information, or any relevant information from database 206 to support its decisions.

Although internet server 112 is also a server system, unlike intranet server 110, it avails some of its services to entities outside of firewall system 116. For instance, internet server 112 may directly receive and respond to email messages from third party organization 120. Thus, when organization property 102 or 102" detaches from private network 114 and as a result loses contact with intranet server

110, one embodiment of a theft prevention system relies on internet server 112 to relocate the property. More particularly, internet server 112 listens for information from theft monitor 106 of the property on outside network 118. Subsequent sections will present examples to elaborate on these servers' roles in a theft prevention system.

Some examples of these discussed server systems are, but not limited to, add-in circuit boards, standalone electronic apparatuses and general-purpose computer systems. A general-purpose computer system 300 is illustrated in Figure 3.

The general-purpose computer system architecture comprises microprocessor 302 and cache memory 306 coupled to each other through processor bus 304. Sample computer system 300 also includes high performance system bus 308 and standard I/O bus 328. Coupled to high performance system bus 308 are microprocessor 302 and system controller 310. Additionally, system controller 310 is coupled to memory subsystem 316 through channel 314, is coupled to I/O controller hub 326 through link 324 and is coupled to graphics controller 320 through interface 322. Coupled to graphics controller is video display 318. Coupled to standard I/O bus 328 are I/O controller hub 326, mass storage 330 and alphanumeric input device or other conventional input device 332.

These elements perform their conventional functions well known in the art. Moreover, it should have been apparent to one ordinarily skilled in the art that

computer system 300 could be designed with multiple microprocessors 302 and may have more components than that which is shown. Also, mass storage 320 may be used to provide permanent storage for the executable instructions of the theft prevention system in one embodiment, whereas memory subsystem 316 may be used to temporarily store the executable instructions during execution by microprocessor 302. In some configurations, mass storage 330 may contain database 206 shown in Figure 2.

OPERATION OF ONE EMBODIMENT OF A THEFT PREVENTION SYSTEM

One embodiment of a theft prevention system handles at least two theft scenarios. Theft scenario 1 involves an individual stealing processor P off validation system V from a quality assurance lab of organization 100. Some assumptions for the purposes of discussing this scenario are: 1) processor P should remain in contact with validation system V at all times unless intranet server 110 modifies its policy engine 202; 2) validation system V has at least one device D capable of providing a unique device identification information; and 3) after the perpetrator removes processor P from validation system V, he or she is still physically within premises of organization 100 and has not had opportunities to reinsert processor P in any other systems. Theft scenario 2 involves an individual stealing notebook computer N from organization 100 for his or her personal use. The assumptions for this scenario are:

1) notebook computer N belongs to a pre-assigned subnet and can assume a range of pre-assigned IP addresses; and 2) the perpetrator uses notebook computer N to logon to the Internet through his or her Internet Service Provider (hereinafter ISP).

Figure 4 illustrates a flow chart of one process that one embodiment of a theft prevention system follows in response to theft scenario 1. Processor P corresponds to organization property 102" and validation system V to electronic system 124 as shown in Figure 1(b). In block 400, the theft prevention system establishes a set of parameters for monitoring properties such as processor P. These monitoring parameters may specify, but not limited to, the amount of time for organization property 102" to remain connected to private network 114 and the type of information exchanges between intranet server 110 and theft monitor 106 of organization property 102". As an illustration, the monitoring parameters may require theft monitor 106 of processor P to transmit or cause to transmit a specifically formatted network packet to intranet server 110 periodically. This network packet contains authentication information related to processor P.

As has been discussed above, authentication of the ownership of processor P can be accomplished by comparing collected identification information and stored identification information relevant to processor P. In one implementation, tamper-resistant storage 104 contains network addresses of intranet server 110 and internet server 112 and a unique device identification information of device D. Theft

monitor 106 sends requests to device D to obtain this identification information. If the collected device identification information does not match the stored one, theft monitor 106 generates a mismatched message that indicates a possible misplacement of processor P. Otherwise, theft monitor 106 generates a matched message.

Then theft monitor 106 proceeds to assemble and transmit an intranet packet with the network address of intranet server 110 as the destination address. Within this packet, theft monitor 106 embeds the matched or mismatched message. In block 402, intranet server 110 parses and analyzes such a network packet. When processor P remains on validation system V, intranet server 110 should observe the matched message in a timely fashion. However, in the event processor P loses contact with validation system V in theft scenario 1, intranet server 110 will not receive the intranet packet from theft monitor 106 within a period of time defined by the previously discussed monitoring parameters. Intranet server 110 thus establishes that theft has occurred and proceeds to alert security personnel 122 shown in Figure 1(b) in block 404.

Security personnel 122 typically stations at entrances or exits of the physical premises of organization 100 and has limited authority to inspect employees' personal belongings. One embodiment of intranet server 110 also has capabilities of identifying a list of employees with access to the lab by accessing employee records in database 206. Intranet server 110 can present the list to security personnel 122 to

thus possibly prevent the perpetrator from leaving the premises of organization 100 with processor P.

As to theft scenario 2, although the process shown in Figure 4 is applicable, one embodiment of a theft prevention system involves additional interactions among theft monitor 106, intranet server 110 and internet server 112. Figure 5 illustrates a flow chart of one process that theft monitor 106 follows to further demonstrate these interactions. Similar to the authentication process described in theft scenario 1, theft monitor 106 also authenticates the ownership of notebook computer N, which corresponds to organization property 102 as shown in Figure 1(a), by comparing appropriate collected identification information and stored identification information in block 500.

More specifically, in one implementation, tamper-resistant storage 104 contains network addresses of intranet server 110 and internet server 112 and a range of IP addresses and subnet information assigned to notebook computer N. Before the perpetrator is able to connect to the Internet through his or her ISP, or third party organization 120 as shown in Figure 1(a), another IP address has to be assigned to notebook computer N. With that in mind, theft monitor 106 searches through configuration information of N for this newly assigned IP address and collects the search outcome. Theft monitor 106 then compares the collected IP address with the information stored in tamper-resistant storage 104. If the collected IP address

neither belongs to the pre-assigned subnet nor falls within the pre-assigned range of IP addresses, theft monitor 106 generates a mismatched message that indicates a possible misplacement of notebook computer N.

Theft monitor 106 also assembles and transmits an intranet packet with the network address of intranet server 110 as the destination address in block 502. Within this packet, theft monitor 106 could embed the mismatched message. In block 504, when intranet server 110 successfully receives the intranet packet, it sends an acknowledgement packet back to theft monitor 106. The acknowledgement packet may instruct theft monitor 106 to continue authenticating the ownership of notebook computer N in a timely manner.

However, because notebook computer N is no longer on private network 114 in theft scenario 2, the intranet packet will not reach intranet server 110. After a certain amount time has lapsed or after a certain number of attempts have been made, theft monitor assembles and transmits an internet packet with the network address of internet server 112 as the destination address in block 506. In the internet packet, theft monitor 106 may embed information representative of its failure to communicate with intranet server 110 and any relevant information indicative of the location of notebook computer N. Some examples of such relevant information are, but not limited to, the newly assigned IP address, the login name of the user, the

name of the ISP, etc. Then theft monitor 106, through network access controller 108, repeatedly transmit these internet packets to internet server 112.

Although specific examples have been provided to illustrate the operations of a theft prevention system, one with ordinary skill in the art may implement the illustrated system without all the disclosed details. For example, instead of assembling either the intranet packet or the internet packet itself, the described theft monitor106 may instruct network access controller 108 or 108" to assemble the packets. An ordinarily skilled artisan may also further divide or combine the functionality of the discussed components of the theft prevention system and establish other monitoring parameters to monitor properties of an organization than the ones disclosed without exceeding the scope of the present invention.

Thus, a method and apparatus for preventing theft of an organization property has been disclosed. Although a theft prevention system has been described particularly with reference to the figures, it may appear in any number of networked systems. It is further contemplated that many changes and modifications may be made by one of ordinary skill in the art without departing from the spirit and scope of the present invention.

CLAIMS

1. A method of preventing theft of an organization property, comprising:
    a. generating an authentication result from comparing stored identification information with collected identification information of the organization property; and
    b. transmitting a plurality types of network packets containing the authentication result to a plurality of organization servers via a network.
2. The method according to claim 1, 1(a) further comprises:
retrieving the stored identification information and network addresses of the organization servers from a tamper-resistant storage location.
3. The method according to claim 2, 1(b) further comprises:
assembling the plurality types of network packets with the network addresses and information indicative of a current location of the organization property.
4. The method according to claim 3, further comprises:
    a. assembling and transmitting an intranet network packet to an intranet server; and
    b. in response to non-acknowledgement from the intranet server, assembling and transmitting an internet network packet to an internet server.
5. The method according to claim 2, further comprises:

retrieving the collected identification information from the organization property.

6. The method according to claim 2, further comprises:

retrieving the collected identification information from an electronic system that contains the organization property.

7. The method according to claim 5, the collected identification information comprises an Internet Protocol address assigned to the organization property.

8. The method according to claim 6, the collected identification information comprises device identification information of the electronic system.

9. A machine readable medium having embodied thereon instructions, which when executed by a machine, causes the machine to prevent theft of an organization property, the instructions comprising:

a. generating a authentication result from comparing stored identification information with collected identification information of the organization property; and

b. transmitting a plurality of network packets that are indicative of the authentication result to a plurality of organization servers via a network.

10. The machine readable medium according to claim 9, the instructions for 9(a) further comprises:

retrieving the stored identification information and network addresses of the organization servers from a tamper-resistant storage location.

11. The machine readable medium according to claim 10, the instructions for 9(b) further comprises:

assembling the plurality types of network packets with the network addresses and information indicative of a current location of the organization property.

12. The machine readable medium according to claim 11, the instructions further including:

a. assembling and transmitting an intranet network packet to an intranet server; and

b. in response to non-acknowledgement from the intranet server, assembling and transmitting an internet network packet to an internet server.

13. The machine readable medium according to claim 10, the instructions further including:

retrieving the collected identification information from the organization property.

14. The machine readable medium according to claim 10, the instructions further including:

retrieving the collected identification information from an electronic system that contains the organization property.

15. The machine readable medium according to claim 13, the collected identification information comprises an Internet Protocol address assigned to the organization property.

16. The machine readable medium according to claim 14, the collected identification information comprises device identification information of the electronic system.

17. A theft prevention system for detecting theft of an organization property, comprising:

a. a plurality of organization servers coupled to a network;

b. a tamper-resistant storage location to maintain stored identification information of the organization property and network addresses of the organization servers;

c. a theft monitor, coupled to the tamper-resistant storage location, to generate a authentication result by comparing stored identification information with collected identification information of the organization property; and

d. a network access controller, coupled to the theft monitor, to transmit a plurality types of network packets containing the authentication result to the organization servers via the network.

18. The theft prevention system according to claim 17, the theft monitor further assembles the plurality types of network packets with the network addresses and information indicative of a current location of the organization property.

19. The theft prevention system according to claim 18, the theft monitor further:

a. transmits an intranet network packet to an intranet server; and

b. in response to non-acknowledgement from the intranet server, transmits an internet network packet to an internet server.

20. The theft prevention system according to claim 18, the theft monitor further:

a. causes the network access controller to transmit an intranet network packet to an intranet server; and

b. in response to non-acknowledgement from the intranet server, causes the network access controller to transmit an internet network packet to an internet server.

21. The theft prevention system according to claim 17, the theft monitor further retrieves the collected identification information from the organization property.

22. The theft prevention system according to claim 17, the theft monitor further retrieves the collected identification information from an electronic system that contains the organization property.

23. The theft prevention system according to claim 21, the collected identification information comprises an Internet Protocol address assigned to the organization property.

24. The theft prevention system to claim 22, the collected identification information comprises device identification information of the electronic system.

ABSTRACT OF THE DISCLOSURE

A method and apparatus for preventing theft of an organization property is disclosed.

In one embodiment, the method and apparatus authenticates the ownership of an organization property by comparing stored identification information with collected identification information of the organization property. Then the method and apparatus transmits multiple types of network packets containing such authentication result to organization servers via a network.

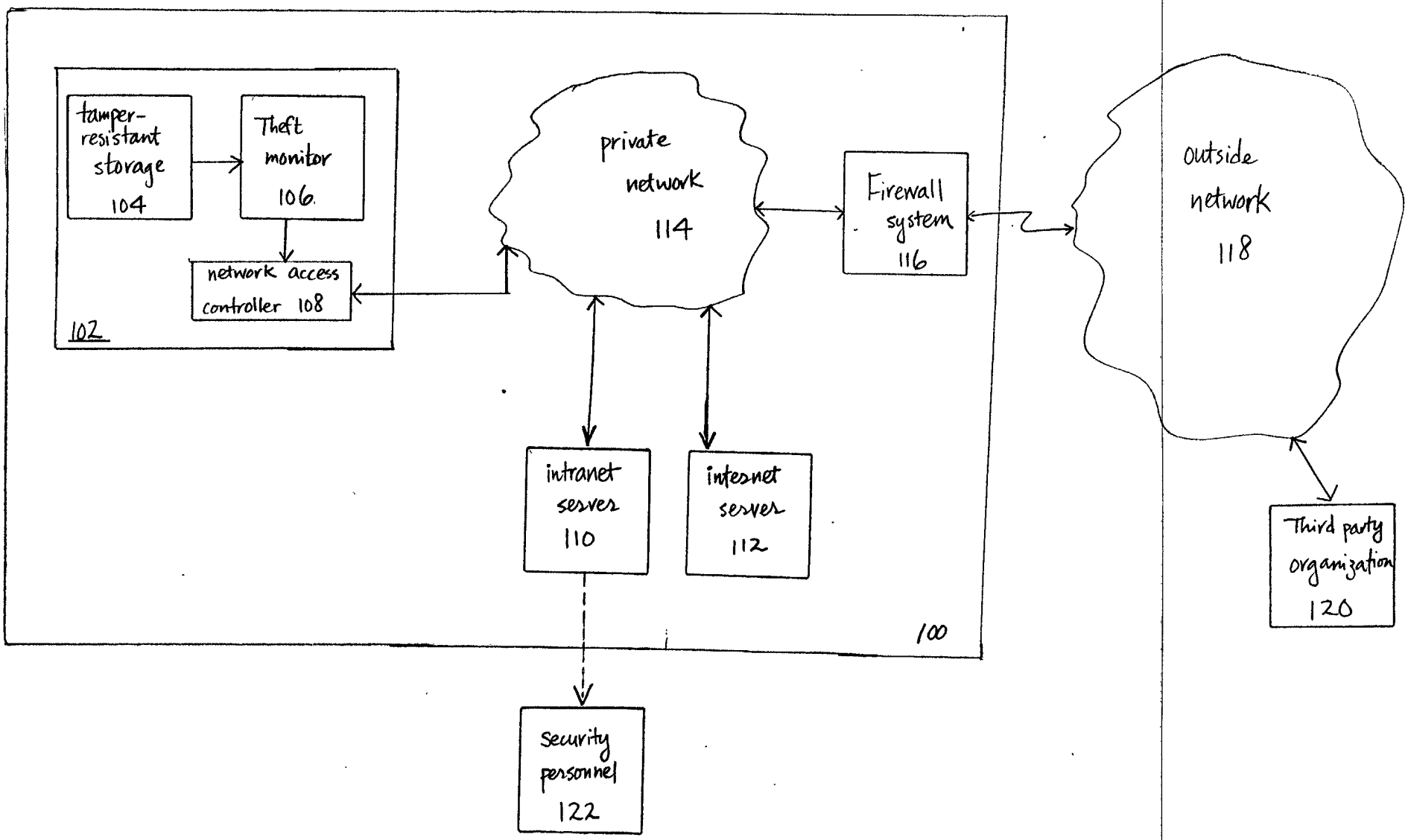
tamper-resistant storage 104
Theft monitor 106
network access controller 108
102
private network 114
Firewall system 116
outside network 118
intranet server 110
internet server 112
Third party organization 120
100
Security personnel 122

Figure 1(a)

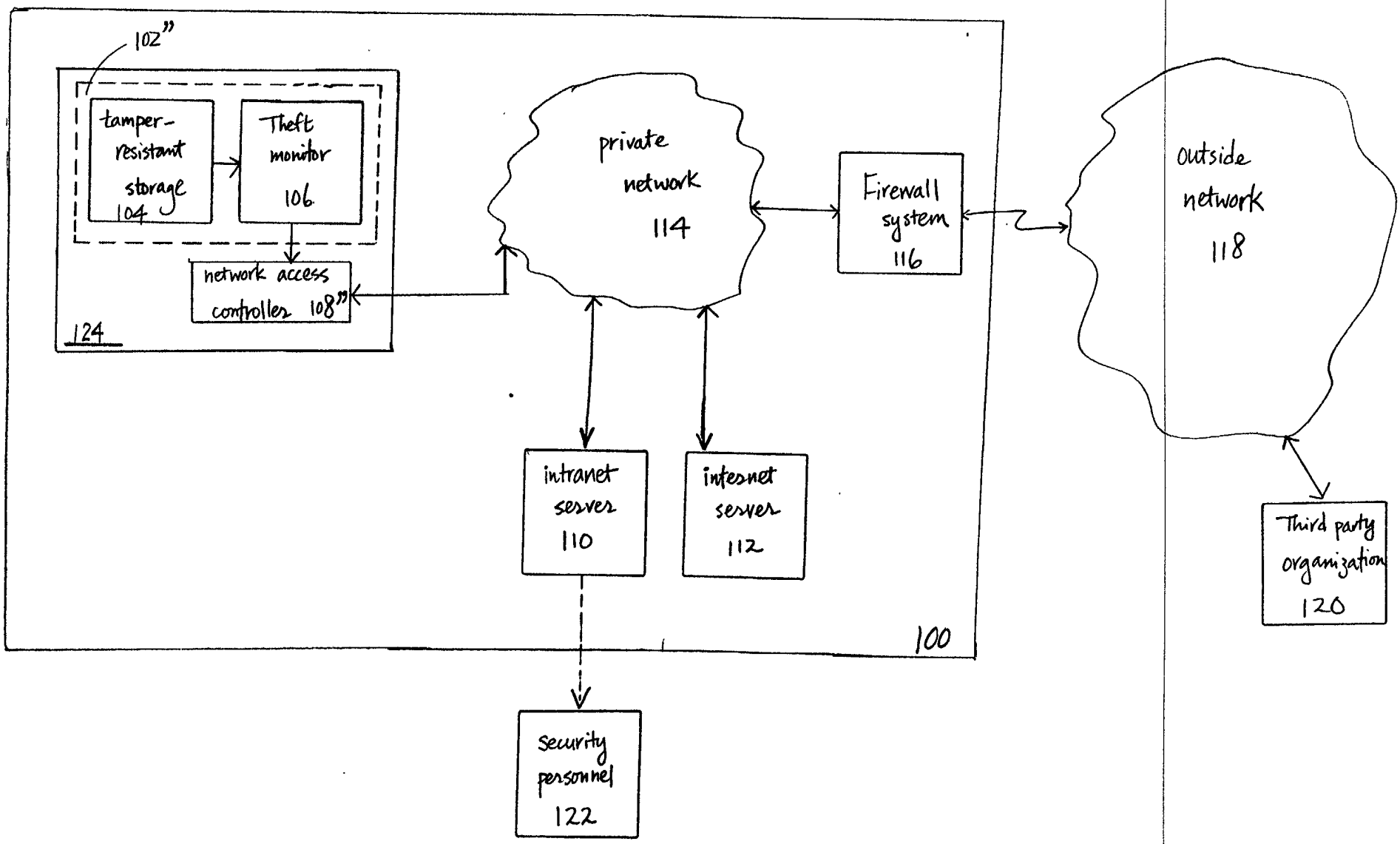
102"
tamper-resistant storage 104
Theft monitor 106
network access controller 108"
124
private network 114
Firewall system 116
outside network 118
intranet server 110
internet server 112
Third party organization 120
100
security personnel 122

Figure 1(b)

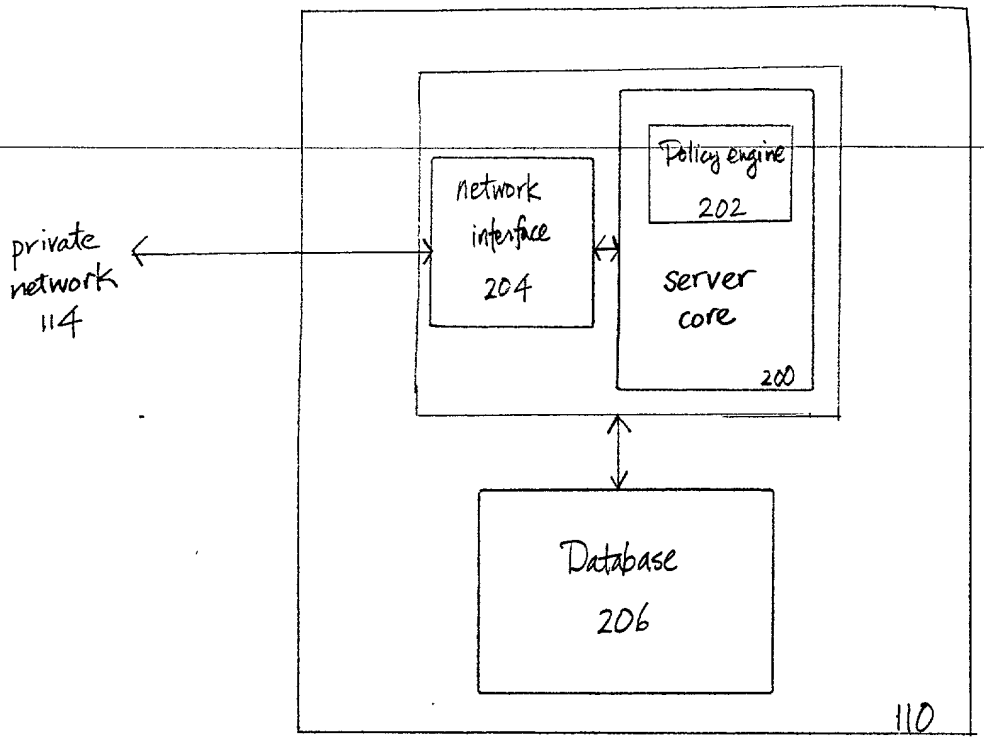
private network 114
network interface 204
Policy engine 202
server core
200
Database 206
110

Figure 2

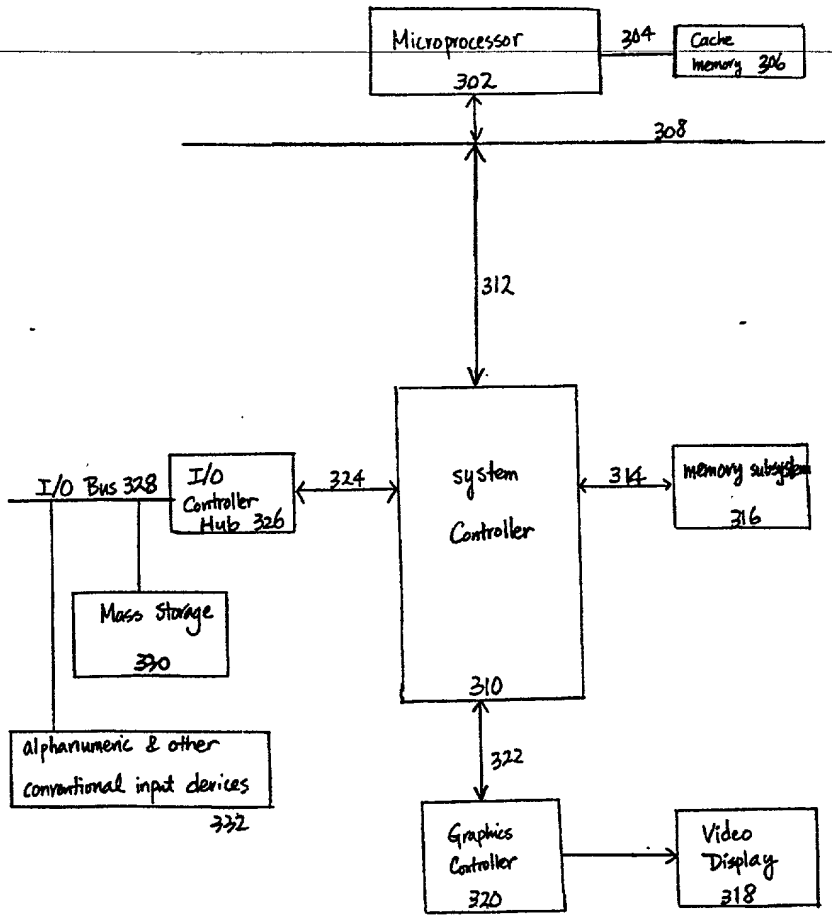
Microprocessor
302
304
Cache memory 306
300
308
312
I/O Bus 328
I/O Controller Hub 326
324
system Controller
314
memory subsystem
316
Mass Storage
330
310
322
Alphanumeric & other conventional input devices
332
Graphics Controller
320
Video Display
318

Figure 3

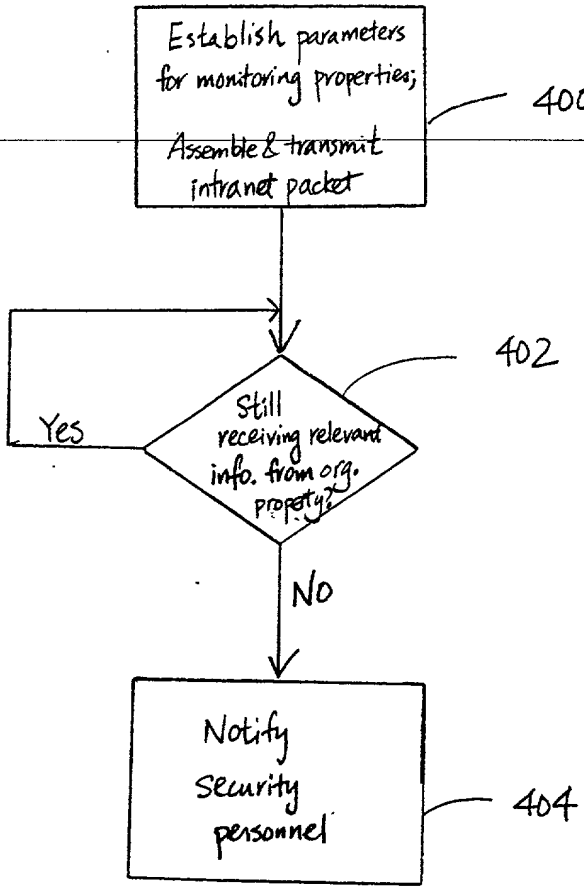
Establish parameters for monitoring properties;
Assemble & transmit intranet packet
400
402
Still receiving relevant info. from org. property?
Yes
No
Notify Security personnel
404

Figure 4

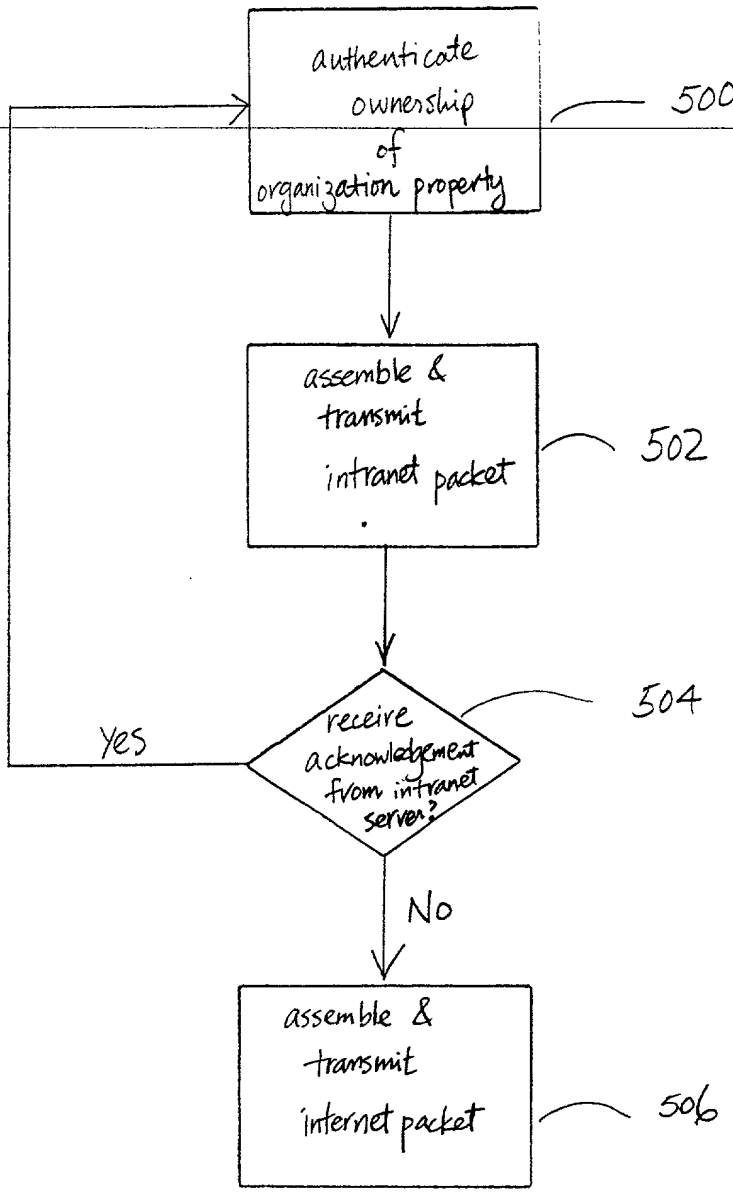
authenticate ownership of organization property
500
assemble & transmit intranet packet
502
receive acknowledgement from intranet server?
504
Yes
No
assemble & transmit internet packet
506

Figure 5

Attorney's Docket No.: 042390.P8731 PATENT

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION
(FOR **INTEL CORPORATION** PATENT APPLICATIONS)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled
METHOD FOR THEFT DETECTION & NOTIFICATION VIA A NETWORK

the specification of which

__xx__ is attached hereto.
___ was filed on _____ as
United States Application Number _____
or PCT International Application Number_____
and was amended on _____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)			Priority Claimed	
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

Application Number	Filing Date
Application Number	Filing Date

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

Application Number	Filing Date	Status -- patented, pending, abandoned
Application Number	Filing Date	Status -- patented, pending, abandoned

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to _____, BLAKELY, SOKOLOFF, TAYLOR &
(Name of Attorney or Agent)
ZAFMAN LLP, 12400 Wilshire Boulevard 7th Floor, Los Angeles, California 90025 and direct telephone calls to _____, (408) 720-8300.
(Name of Attorney or Agent)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor Thomas L. Stachura

Inventor's Signature _____ Date _____

Residence Portland, Oregon (City, State) Citizenship India (Country)

Post Office Address 15016 NW Blakely Lane
Portland, Oregon 97229

Full Name of Second/Joint Inventor Anil Vasudevan

Inventor's Signature _____ Date _____

Residence Portland, Oregon (City, State) Citizenship U.S.A. (Country)

Post Office Address 12849 NW Marshall Court
Portland, Oregon 97229

Full Name of Third/Joint Inventor _____

Inventor's Signature _____ Date _____

Residence _____ (City, State) Citizenship _____ (Country)

Post Office Address _____

Full Name of Fourth/Joint Inventor _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

Post Office Address _____
_____

Full Name of Fifth/Joint Inventor _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

Post Office Address _____
_____

Full Name of Sixth/Joint Inventor _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

Post Office Address _____
_____

Full Name of Seventh/Joint Inventor _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

Post Office Address _____
_____

APPENDIX A

William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. P42,261; Aloysius T. C. AuYeung, Reg. No. 35,432; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; Gregory D. Caldwell, Reg. No. 39,926; Andrew C. Chen, Reg. No. 43,544; Thomas M. Coester, Reg. No. 39,637; Alin Corie, Reg. No. P46,244; Dennis M. deGuzman, Reg. No. 41,702; Stephen M. De Klerk, under 37 C.F.R. § 10.9(b); Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Sanjeet Dutta, Reg. No. P46,145; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; Paramita Ghosh, Reg. No. 42,806; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Willmore F. Holbrow III, Reg. No. P41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; William W. Kidd, Reg. No. 31,772; Sang Hui Kim, Reg. No. 40,450; Eric T. King, Reg. No. 44,188; Erica W. Kuo, Reg. No. 42,775; Kurt P. Leyendecker, Reg. No. 42,799; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Chun M. Ng, Reg. No. 36,878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Daniel E. Ovanezian, Reg. No. 41,236; Marina Portnova, Reg. No. P45,750; Babak Redjaian, Reg. No. 42,096; William F. Ryann, Reg. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey Sam Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; John F. Travis, Reg. No. 43,203; George G. C. Tseng, Reg. No. 41,355; Joseph A. Twarowski, Reg. No. 42,191; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Mark L. Watson, Reg. No. P46,322; Thomas C. Webster, Reg. No. P46,154; Charles T. J. Weigell, Reg. No. 43,398; Steven D. Yates, Reg. No. 42,242; and Norman Zafman, Reg. No. 26,250; my patent attorneys, and Justin M. Dillon, Reg. No. 42,486; my patent agent, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and Alan K. Aldous, Reg. No. 31,905; Robert D. Anderson, Reg. No. 33,826; Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468; Jeffrey S. Draeger, Reg. No. 41,000; Cynthia Thomas Faatz, Reg No. 39,973; Sean Fitzgerald, Reg. No. 32,027; John N. Greaves, Reg. No. 40,362; Seth Z. Kalson, Reg. No. 40,670; David J. Kaplan, Reg. No. 41,105; Charles A. Mirho, Reg. No. 41,199; Leo V. Novakoski, Reg. No. 37,198; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; Kenneth M. Seddon, Reg. No. 43,105; Mark Seeley, Reg. No. 32,299; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Steven C. Stewart, Reg. No. 33,555; Raymond J. Werner, Reg. No. 34,752; Robert G. Winkle, Reg. No. 37,474; and Charles K. Young, Reg. No. 39,435; my patent attorneys, and Thomas Raleigh Lane, Reg. No. 42,781; Calvin E. Wells; Reg. No. P43,256, Peter Lam, Reg. No. 44,855; and Gene I. Su, Reg. No. 45,140; my patent agents, of INTEL CORPORATION; and James R. Thein, Reg. No. 31,710, my patent attorney; with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

APPENDIX B

Title 37, Code of Federal Regulations, Section 1.56
Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclosure information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclosure all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) Prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made or record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application;

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.